

What does the normalization of preemptive US cyberattacks mean for the stability of international norms regarding sovereign digital territory and the long-term risk of uncontrolled escalation in critical infrastructure?

September 8, 2026 | SnugLab Research

Executive Summary

The normalization of preemptive US cyberattacks, particularly through "Defend Forward" operations, destabilizes international norms regarding sovereign digital territory and heightens the long-term risk of uncontrolled escalation in critical infrastructure. While intended to deter malicious activity and clarify strategic red lines, the evidence suggests these operations erode the principle of digital inviolability by creating a "liability gap" for low-intensity intrusions and fostering operational ambiguity that forces adversaries into worst-case interpretations, increasing the potential for miscalculation and conflict [9, 13].

Key Findings

Divergent Interpretations of Sovereign Digital Territory

A fundamental challenge to international norms stems from the lack of a universally agreed-upon definition for "sovereign digital territory" and the threshold for its violation [3, 11]. The United States, aligning with its "Defend Forward" strategy, operates under a high threshold, asserting that cyber operations only violate sovereignty if they cause physical damage, injury, loss of functionality requiring repair, or interfere with inherently governmental functions [3, 6, 11, 12]. The US Department of Defense views sovereignty as a "baseline principle" rather than a primary rule that automatically triggers international legal responsibility for every intrusion [6]. This high threshold allows the US to conduct persistent, low-intensity cyber operations, such as planting malware in foreign electrical grids, without immediately breaching international law regarding territorial inviolability [5, 6, 8].

Conversely, several major powers and international bodies, including France, Iran, and the African Union, advocate for a lower threshold, where any unauthorized penetration or

unlawful intrusion into foreign ICT infrastructure constitutes a sovereignty violation [10, 12]. The African Union explicitly rejects a *de minimis* bar for unauthorized access [12]. This divergence creates normative ambiguity, as US preemptive intrusions, considered permissible by US doctrine, may be interpreted as hostile acts by states adhering to a lower threshold, exacerbating the security dilemma [6, 9].

Erosion of Norms Versus Stabilization Through Deterrence

The normalization of US "Defend Forward" operations presents a tension between eroding sovereign digital inviolability and stabilizing international order. Proponents argue that these operations stabilize order by establishing credible deterrence and clarifying strategic red lines. By proactively imposing costs on adversaries and disrupting malicious activity at its source, the US aims to prevent malign actors from operating with impunity and signal resolve [9, 13]. This approach can act as a "cross-domain release valve," allowing states to respond to provocations through cyber means without immediately escalating to kinetic conflict [9].

However, critics contend that this strategy fundamentally erodes traditional notions of territorial sovereignty. By routinely operating on non-US networks, the US challenges the "sovereignty-as-rule" view held by many states, which considers any unauthorized penetration a violation [4, 6, 10]. This unilateral enforcement creates a "liability gap" where low-intensity operations inflict cumulative harm without clear legal consequences or collective enforcement, potentially fostering a chaotic environment for digital territory [9, 13].

Escalation Risk from Operational Ambiguity in Critical Infrastructure

The persistent blending of espionage and pre-positioned malware in foreign networks systematically raises the risk of uncontrolled escalation, particularly in critical infrastructure. US "Defend Forward" strategies involve routinely planting malware and maintaining non-destructive access in foreign systems [1, 9]. Adversaries face significant difficulty distinguishing between routine intelligence gathering and preparatory operations for a disabling strike on critical infrastructure because these persistent intrusions are structurally identical [9].

This operational ambiguity forces adversaries into worst-case interpretations. Detecting US malware in their power grids or military networks may lead adversaries to interpret all persistent cyber operations as escalatory, intensifying the security dilemma and

increasing the likelihood of inadvertent escalation [9]. Critical infrastructure sectors, such as energy grids, are highly interdependent and vulnerable, meaning a misinterpreted cyber operation could quickly trigger kinetic responses or broader conflict [2, 8]. The absence of widely accepted norms to clarify the threshold between espionage and preparation ensures that miscalculation remains a constant threat to international stability [2, 9].

Targeted Critical Infrastructure and Malware Capabilities

Publicly available information on specific foreign critical infrastructure sectors targeted by US "Defend Forward" pre-positioning operations is limited due to the classified nature of these activities [13]. However, one notable documented instance involves the Russian electrical grid. In 2019, American hackers from US Cyber Command reportedly planted malware capable of disrupting power generation or distribution within this sector [5]. Other offensive cyber operations include targeting ISIS networks and disrupting the Russian Internet Research Agency's network access during the 2018 U.S. midterm elections [13]. While US Cyber Command has deployed "hunt forward" teams to Ukraine to defend critical infrastructure, specific details on other foreign sectors frequently targeted by US pre-positioning malware in the last five years are not publicly detailed [13].

Status of International Legal Consensus on Cyber Thresholds

There is no single, universally agreed-upon international legal consensus or formal treaty defining the precise threshold for cyber-induced physical damage versus mere functional disruption [3, 11]. However, there is broad agreement that cyber operations causing physical damage, injury, or a loss of functionality requiring repair or replacement of cyber infrastructure constitute a violation of sovereignty [3, 6, 11, 12]. Most states, including the US, apply a consequence-based approach, using a "scale and effects test" to determine if impacts are comparable to traditional uses of force [3, 7, 11].

Despite this, France, Iran, and the African Union explicitly reject the US's high-threshold interpretation. They advocate for a lower threshold, asserting that any unauthorized penetration or unlawful intrusion into ICT infrastructure on foreign territory constitutes a sovereignty violation [10, 12]. The African Union specifically rejects a *de minimis* threshold for unauthorized access [12]. UN Group of Governmental Experts (GGE) reports from 2013, 2015, and 2021 consistently affirm the application of state sovereignty to ICT activities, but do not resolve this definitional divergence [10].

Documented Escalation Risks

While the research identifies a recognized structural risk of misinterpretation leading to escalation, it does not document a specific case study where an adversary state explicitly misinterpreted non-destructive US espionage or pre-positioning as an imminent kinetic attack, leading to measurable escalation in critical infrastructure. The difficulty adversaries face in distinguishing between routine cyber espionage and more destructive degradation operations is highlighted as a key factor exacerbating the security dilemma and raising the potential for inadvertent escalation [9].

Implications

The normalization of preemptive US cyberattacks has significant implications for international stability. The US's high-threshold interpretation of digital sovereignty, coupled with its "Defend Forward" strategy, creates a persistent "grey zone" of activity that challenges the foundational international norm of sovereign inviolability [6, 9, 13]. This unilateral assertion of operational freedom, while intended to deter, risks fostering a less predictable and more volatile international environment where states operate under conflicting legal frameworks [3, 11].

The persistent blending of espionage and pre-positioning malware in critical infrastructure networks means that adversaries are systematically forced to assume the worst, increasing the likelihood of miscalculation [9]. This operational ambiguity, combined with the lack of universal norms, heightens the long-term risk of uncontrolled escalation, potentially leading to kinetic responses or broader conflict triggered by cyber incidents [2, 9]. For international norms to stabilize, greater consensus on the definition of digital sovereignty and clear thresholds for permissible cyber operations are necessary to reduce the inherent risks of this proactive cyber posture.

Limitations and Caveats

The analysis is limited by the inherent opacity of offensive cyber operations, particularly those conducted by state actors. Specific details regarding the frequency, targets, and capabilities of US pre-positioning malware in foreign critical infrastructure sectors are largely classified, making comprehensive assessment challenging [13]. While the research identifies a strong theoretical risk of misinterpretation leading to escalation, specific documented case studies of such events are not available in the provided

findings. The differing interpretations of "sovereignty" and "use of force" in cyberspace among states further complicate the assessment of normative stability.

Sources

- [1] [gov] United States International Cyberspace And Digital Policy St - 2021-2025.state.gov - <https://2021-2025.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/>
- [2] [gov] 2009-2017.state.gov - <https://2009-2017.state.gov/t/avc/rls/264756.htm>
- [3] [edu] Evolving Interpretation Use Of Force Cyber Operations Insigh - lieber.westpoint.edu - <https://lieber.westpoint.edu/evolving-interpretation-use-of-force-cyber-operations-insights-state-practices/>
- [4] [edu] Viewcontent.Cgi - digital-commons.usnwc.edu - <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2987&context=ils>
- [5] [wiki] Cyberwarfare And The United States - en.wikipedia.org - https://en.wikipedia.org/wiki/Cyberwarfare_and_the_United_States
- [6] Respect Sovereignty Cyberspace - texaslawreview.org - <https://texaslawreview.org/respect-sovereignty-cyberspace/>
- [7] [peer-reviewed] A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice - Authors: Dan Efrony; Yuval Shany - Journal: American Journal of International Law - <https://www.cambridge.org/core/journals/american-journal-of-international-law/article/rule-book-on-the-shelf-tallinn-manual-20-on-cyberoperations-and-subsequent-state-practice/54FBA2B30081B53353B5D2F06F778C14>
- [8] Cyber Effects In Warfare Categorizing The Where What And Why - tnsr.org - <https://tnsr.org/2024/08/cyber-effects-in-warfare-categorizing-the-where-what-and-why/>
- [9] [commentary] Myth Cyber Offense Case Restraint - cato.org - <https://www.cato.org/policy-analysis/myth-cyber-offense-case-restraint>
- [10] wicinternet.org - https://www.wicinternet.org/2024-01/16/c_956165.htm
- [11] Cyber Space Sovereignty And The Intricacies Of International - voelkerrechtsblog.org - <https://voelkerrechtsblog.org/cyber-space-sovereignty-and-the-intricacies-of-international-law-making/>
- [12] Sovereignty - cyberlaw.ccdcoe.org - <https://cyberlaw.ccdcoe.org/wiki/Sovereignty>
- [13] [edu] Viewcontent.Cgi - repository.law.miami.edu - <https://repository.law.miami.edu/cgi/viewcontent.cgi?article=2614&context=umialr>